УДК 389:14:621.317:354
DOI: 10.15587/1729-4061.2019.154352

Випробування програмного забезпечення засобів вимірювальної техніки з метою оцінки відповідності

О. М. Величко, В. В. Гаман, Т. Б. Гордієнко, О. В. Грабовський

Проведено аналіз нормативної бази з випробування програмного забезпечення (ПЗ) для засобів вимірювальної техніки (ЗВТ) на національному рівні з метою встановлення її придатності для здійснення оцінювання відповідності. Здійснено порівняння загальних вимог національних нормативних документів та документів міжнародних і регіональних організацій законодавчої метрології OIML та WELMEC. Зокрема стосовно придатності ПЗ до застосування та захисту від несанкціонованого втручання. Встановлено, що чинний національний стандарт містить лише загальні вимоги щодо захисту ПЗ та не визначає методології проведення випробувань ПЗ. Це важливо, оскільки ЗВТ, призначені для застосування у сфері законодавчо регульованої метрології, повинні проходити процедуру оцінювання відповідності вимогам технічних регламентів.

Визначено основні відмінності та встановлені необхідні елементи для досягнення презумпції відповідності ПЗ суттєвим вимогам технічних регламентів під час оцінювання відповідності ЗВТ. Оцінено вимоги нормативних документів стосовно придатності до застосування та захисту від несанкціонованого втручання. Для конкретизації вимог до ПЗ і забезпечення виконання вимог методики випробувань ПЗ встановлено необхідність додаткового використання вимог документів OIML D 31 і WELMEC 7.2. Доведена потреба перегляду чинного національного стандарту щодо випробування ПЗ для ЗВТ. Встановлений та досліджений алгоритм проведення випробувань ПЗ ЗВТ з метою оцінки відповідності. Алгоритм враховує вимоги міжнародних стандартів щодо життєвого циклу ПЗ і щодо системи якості під час розробки ПЗ. Це дозволить врахувати всі елементи, необхідні для досягнення презумпції відповідності ПЗ суттєвим вимогам технічних регламентів

Ключові слова: програмне забезпечення, засіб вимірювальної техніки, випробування, оцінка відповідності, технічний регламент

1. Вступ

В умовах майже універсального використання інформаційних технологій (ІТ) все більшу роль відіграє спеціалізоване програмне забезпечення (ПЗ) для засобів вимірювальної техніки (ЗВТ). Відповідно до Закону України «Про метрологію та метрологічну діяльність» ЗВТ, призначені для застосування у сфері законодавчо регульованої метрології, повинні проходити процедуру оцінювання відповідності вимогам технічних регламентів (ТР).

Оцінювання відповідності є процесом доведення того, що суттєві вимоги ТР, які стосуються ЗВТ, були виконані. При оцінюванні відповідності ЗВТ ви-

сувають наступні суттєві вимоги, що так чи інакше стосуються ПЗ: придатність до застосування та захист від несанкціонованого втручання.

Згідно із національним законодавством сформовані переліки національних стандартів, відповідність яким, зокрема, надає презумпцію відповідності ЗВТ суттєвим вимогам ТР. Тому наразі актуальним є аналіз стану нормативної бази щодо випробування ПЗ для ЗВТ і розроблення підходів до узгодження відповідних документів на національному рівні. При цьому доцільно враховувати документи та рекомендації міжнародних і регіональних організацій, що займаються питаннями законодавчої метрології.

Правила і процедури випробувань ПЗ для ЗВТ встановлені документом [1] Міжнародної організації законодавчої метрології (OIML), а також документами та рекомендаціями регіональних метрологічних організацій. Зокрема процедури випробувань ПЗ для ЗВТ регламентуються рекомендацією [2] Євразійського співробітництва державних метрологічних закладів (COOMET), документом [3] і настановою [4, 5] Європейської організації зі співробітництва в сфері законодавчої метрології (WELMEC).

Актуальність роботи підтверджується нагальною необхідністю проводити оцінювання відповідності законодавчо регульованих ЗВТ відповідно до вимог національного законодавства, ТР або європейських директив. У більшості випадків ПЗ є одним з ключових компонентів таких ЗВТ. Тому національні метрологічні інститути та органи з оцінювання відповідності зацікавлені у наявності дієвих методів випробувань ПЗ ЗВТ, оцінювання ризиків і загроз, пов’язаних з застосуванням. Зважаючи на це, актуальним питанням є дослідження стану нормативної бази щодо випробувань ПЗ для ЗВТ на національному рівні та встановлення необхідних елементів для досягнення презумпції відповідності ПЗ вимогам ТР під час оцінювання відповідності ЗВТ.

2. Аналіз літературних даних та постановка проблеми

На сьогодні важливим і складним завданням є трансформація національної метрологічної нормативної бази і її гармонізація з документами, рекомендаціями та стандартами відповідних міжнародних організацій. Саме OIML сприяє глобальній гармонізації законодавчих метрологічних процедур. Нормативна база національної метрологічної служби, правила, технічна та організаційна база в Україні визначаються законодавством України про метрологію. Зокрема, вимоги Європейської Директиви 2014/32/ЄС про вимірювальні прилади (MID) [6] є основою законодавства України щодо оцінювання відповідності ЗВТ.

Ґрунтовний аналіз щодо ПЗ для ЗВТ було предметом попередніх досліджень авторів [7–11]. В [7, 8] досліджено особливості нормативного забезпечення випробувань ПЗ ЗВТ. Основні етапи випробування ПЗ ЗВТ і особливості відповідно до вимог [1, 4, 5] розглянуто в [9]. Використання валідованого ПЗ для оцінювання невизначеності вимірювань у акредитованих лабораторіях представлено в [10]. Розглянуті основні фактори та алгоритми щодо випробування ПЗ для ЗВТ згідно з вимогами OIML і WELMEC, запропоновано універсальний алгоритм випробування ПЗ для ЗВТ у [11]. Однак, ці дослідження не містять аналізу вимог та особливостей міжнародних і регіональних документів

[1, 4, 5] з метою спільного впровадження у національних стандартах з питань випробування ПЗ для ЗВТ.

В [12–17] розглянуті питання безпеки, оцінювання ризиків та поточних загроз, пов'язаних із застосуванням ПЗ ЗВТ, у т. ч. тих, які інтегровані у відкриті мережі. Ці дослідження зосереджені на методах, які враховують вимоги регіональних настанов [4, 5] та міжнародних стандартів. Однак у [12–16] не враховані вимоги міжнародного документа [1] та можливість застосування ПЗ для локальних ЗВТ, а положення, викладені у [17], застосовні виключно до систем інтелектуального вимірювання.

У [18] розглянуто класи ризику ПЗ, настанова з підтвердження та деякі можливі методи випробувань ПЗ для локальних ЗВТ відповідно до вимог [1, 4, 5]. Однак у роботі не розглянуто можливість випробувань ПЗ ЗВТ, інтегрованих у відкриті мережі. У [19] запропоновано підхід, спрямований на автоматичну перевірку параметрів для ПЗ, вбудованих у ЗВТ відповідно до вимог міжнародного документа [1]. Розглянуті загальні критерії для оцінювання безпеки та захисту компонентів ІТ. Однак робота не враховує вимоги регіональних настанов [4, 5].

Таким чином, можна зробити висновок, що у проведених дослідженнях не аналізувались можливості адаптації або спільного застосування положень міжнародних і регіональних документів [1, 4, 5] з випробування ПЗ для ЗВТ. Також не досліджувалась ступінь інтеграції цих вимог у національні нормативні стандарти.

Тому, стан нормативної бази випробування ПЗ для ЗВТ вимагає більш детального аналізу на предмет наявності необхідних елементів, зокрема встановлених у міжнародному документі [1] та регіональних рекомендаціях [4, 5], для досягнення презумпції відповідності ПЗ вимогам ТР під час оцінювання відповідності ЗВТ. Таке дослідження необхідно здійснити для визначення доцільності актуалізації національної нормативної бази щодо випробувань ПЗ ЗВТ або додаткового використання методології, викладеної у документах міжнародних і регіональних організацій.

3. Мета та задачі дослідження

Проведені дослідження ставили за мету розробити підходи щодо гармонізації вимог документів міжнародних і регіональних метрологічних організацій щодо випробування спеціального ПЗ ЗВТ на національному рівні.

Для досягнення поставленої мети вирішувалися наступні задачі:

– здійснити аналіз положень національних нормативних документів щодо випробування ПЗ ЗВТ на відповідність суттєвим вимогам технічних регламентів та порівняти з вимогами, викладеними в документах міжнародних та регіональних організацій;

– встановити і дослідити необхідні елементи, достатні для досягнення презумпції відповідності ПЗ суттєвим вимогам технічних регламентів під час оцінювання відповідності ЗВТ, особливо щодо придатності ПЗ до застосування та захисту від несанкціонованого втручання;

– встановити і дослідити алгоритм проведення випробувань ПЗ ЗВТ з метою оцінки відповідності.

4. Матеріали та методи дослідження щодо застосування програмного забезпечення засобів вимірювальної техніки

Захист ПЗ в широкому сенсі є комплексом заходів, спрямованих на запобігання несанкціонованого використання, вивчення, поширення та модифікування ПЗ, а також захист від випадкового втручання. Для ПЗ ЗВТ важливими є захист від несанкціонованого модифікування ПЗ та його компонентів, вимірювальних даних, захист від ненавмисних та випадкових втручань, а саме:

– вихідний код ПЗ;

– вимірювальні дані з датчиків вимірювальної системи;

– команди, що вводить користувач;

– вимірювальні дані, що виводяться на дисплей;

– вимірювальні дані та калібрувальні коефіцієнти, що зберігаються в довготривалій пам’яті приладу;

– вимірювальні дані, що передаються по каналам зв’язку.

Залежно від типу побудови ЗВТ, з вбудованим ПЗ (рис. 1) або на базі універсального комп’ютера (рис. 2), використовуються різні підходи та заходи щодо захисту ПЗ, його компонентів та даних.

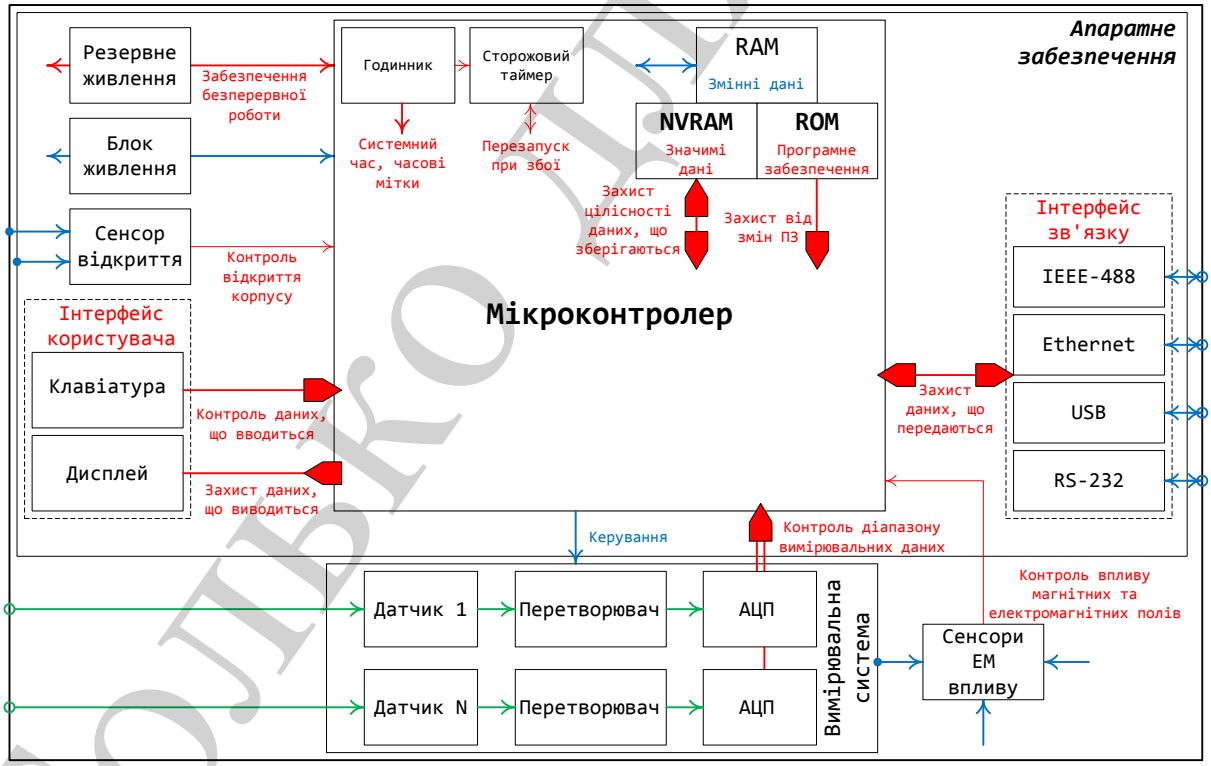

Рис. 1. Структурна схема ЗВТ з вбудованим ПЗ

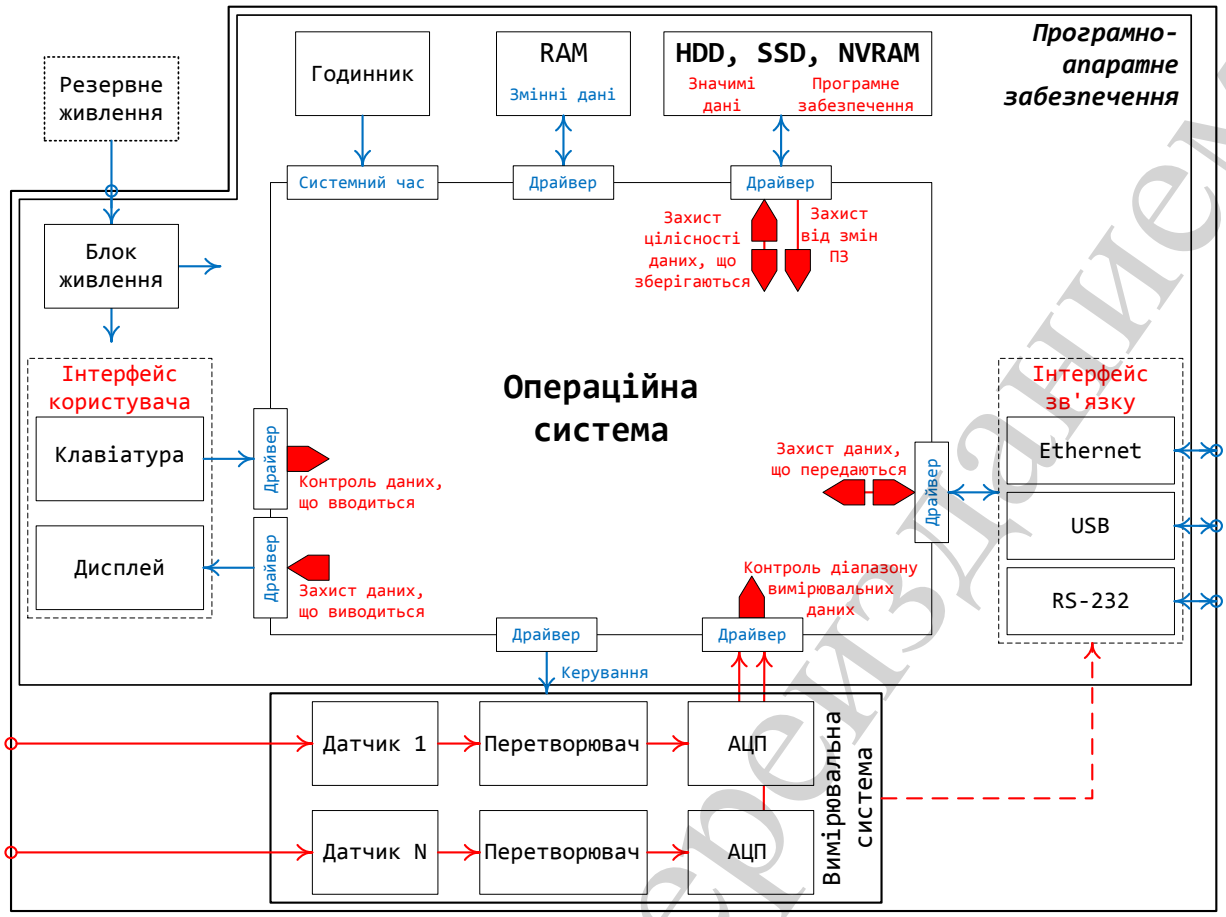

Рис. 2. Структурна схема ЗВТ на базі універсального комп’ютера

ЗВТ з вбудованим ПЗ мають такі основні особливості:

– вони реалізуються тільки для здійснення конкретних вимірювань, встановлених виробником;

– вони містять мікроконтролер з фіксованим набором команд і необхідними для роботи компонентами;

– з його панелі можуть вводитись тільки команди, встановлені виробником;

– на його дисплеї відображається тільки встановлена виробником інформація;

– можуть використовуватися тільки встановлені виробником інтерфейси зв’язку;

– вимірювальна та апаратна частини розміщуються у захисному корпусі, який може бути фізично захищеним.

Зазначені особливості надають такі можливості для забезпечення захисту як ПЗ, так і ЗВТ загалом:

– можливе апаратне блокування перезапису вбудованого ПЗ;

– застосування спеціалізованих мікроконтролерів з вбудованими каналами аналого-цифрового перетворення (АЦП) дозволяє вводити дані вимірювань з датчиків чи перетворювачів одразу до мікроконтролера, що виключає можливість втручання в них;

– можливе використання мікроконтролерів з вбудованими спеціалізованими модулями для забезпечення захисту;

– неможливо без втручання в апаратну частину приладу зіпсувати дані та команди, що передаються між мікроконтролером та інтерфейсом користувача;

– мікроконтролер містить необхідний об'єм внутрішньої постійної, оперативної та енергонезалежної пам'яті;

– відсутні механізми втручання в дані, що зберігаються, ніж ті, що встановив виробник;

– при збоях роботи ЗВТ, пов'язаних з ПЗ, можливий його перезапуск за командою сторожового таймера;

– через інтерфейси зв'язку передаються тільки визначені виробником команди та дані, пов'язані з процесом вимірювання;

– у разі відкриття корпусу ЗВТ чи при спрацюванні датчиків магнітного та електромагнітного полів біля чутливих елементів вимірювальної системи створюються відповідні записи у його журналі подій.

ЗВТ на базі універсального комп'ютера мають такі основні особливості:

– вони реалізуються для здійснення конкретних вимірювань, однак вони можуть бути запрограмовані також для здійснення інших вимірювань;

– обробка вимірювальних даних, зберігання та передача виміряних значень відбувається за допомогою універсального комп'ютера, який працює під керуванням певної операційної системи;

– можливе виконання на універсальному комп'ютері також і інших задач з введенням будь-яких даних одночасно з процесом вимірювання;

– можливе відображення на дисплеї універсального комп'ютера інформації, вибраної користувачем і не пов'язаної з процесом вимірювання;

– можуть використовуватися інтерфейси зв'язку, передбачені виробником універсального комп'ютера, які можуть не використовуватися в процесі вимірювання чи передачі вимірювальних даних;

– вимірювальна та програмно-апаратна частини можуть бути розміщені як в одному, так і у різних корпусах, і це не гарантує захисту від втручання в ПЗ.

Зазначені особливості вимагають такі заходи для забезпечення захисту ПЗ:

– для забезпечення цілісності ПЗ необхідно перевіряти контрольні суми його значимих файлів;

– необхідно здійснювати контроль даних з вимірювальної системи, особливо тоді, коли ці дані надходять через інтерфейс зв'язку;

– необхідні заходи щодо обмеження прав доступу користувача до ресурсів ПЗ, операційної системи, за необхідності;

– індикація вимірювальних даних повинна бути в пріоритеті в процесі вимірювання;

– для захисту вимірювальних та інших значимих даних, що зберігаються, можливе використання контрольних сум для перевірки цілісності даних та дублювання даних для відновлення при їх псуванні;

– необхідне здійснення контролю даних та команд, що передаються через інтерфейси зв'язку, для унеможливлення несанкціонованого впливу на роботу ПЗ ЗВТ;

– необхідно забезпечити захист даних, що передаються між значимою та не значимою частинами ПЗ ЗВТ;

– можуть бути задіяні механізми перевірки ідентифікації, справжності та цілісності даних при оновленні ПЗ з можливістю відмови від оновлення ПЗ і повернення до попередньої версії;

– необхідне використання зовнішнього джерела безперервного живлення для забезпечення безперервної роботи ЗВТ.

ПЗ ЗВТ, що має необхідний рівень захисту, є захищеним.

ПЗ повинно бути розроблене таким чином, щоб забезпечити максимальну придатність до правильного застосування ЗВТ, в т. ч.:

– не мати не задокументованих функцій чи команд, які можуть впливати на метрологічні характеристики або працездатність ЗВТ;

– виключити навмисні чи ненавмисні дії користувача через інтерфейси, які можуть спотворювати результати вимірювань.

Вказані вимоги відносяться до ПЗ, якщо воно може впливати на результати вимірювань, зберігання або передачу результатів вимірювань. Це може бути як основне ПЗ ЗВТ (вбудоване або універсальне), так і додаткове або допоміжне ПЗ, що використовується для обробки результатів вимірювань.

Додаткове (допоміжне) ПЗ також повинно бути ідентифіковане і захищене, тобто для нього необхідно провести таку ж саму процедуру випробувань, як і для основного ПЗ. Виробники ЗВТ з ПЗ повинні надати всю необхідну інформацію, що стосується ідентифікації ПЗ, прийнятих заходів для забезпечення захисту та придатності ПЗ.

Для перевірки відповідності вимогам до ПЗ ЗВТ можливе застосування стандарту ДСТУ 7363 [20], який включено до переліку національних стандартів, відповідність яким надає презумпцію відповідності ЗВТ суттєвим вимогам ТР щодо ЗВТ.

Документ OIML D 31 [1] рекомендований до застосування в країнах-членах OIML під час затвердження типу ЗВТ з програмним керуванням. Для перевірки відповідності ПЗ ЗВТ вимогам Директиви MID [6] розроблено спеціальну рекомендацію WELMEC 7.2 [4].

5. Загальні вимоги міжнародних і регіональних документів щодо програмного забезпечення для засобів вимірювальної техніки

Документ OIML D 31 [1] встановлює загальні вимоги до ЗВТ з програмним керуванням. Вимоги документу не охоплюють всі технічні вимоги, що є індивідуальними для кожної категорії ЗВТ. Ці вимоги повинні бути викладені у відповідних нормативно-правових документах. Основним об’єктом документу є ЗВТ з ПЗ.

Вимоги до ЗВТ поділяють на такі:

– основні вимоги, що стосуються ідентифікації ПЗ і правильності застосованих алгоритмів, функцій;

– вимоги по захисту ПЗ (попередження випадкового неправильного застосування ЗВТ і захист від шахрайства);

– вимоги щодо підтримки апаратних засобів при виявленні помилок для забезпечення надійності роботи ЗВТ з ПЗ;

– спеціальні вимоги для окремих конфігурацій залежно від сфери застосування ЗВТ:

– визначення і розділення апаратної та програмної частини на законодавчо значимі та не значимі, виділення контрольованих частин та їх інтерфейсів;

– забезпечення сумісного відображення та друку інформації законодавчо значимих та не значимих частин; зберігання даних та передача по мережам зв'язку;

– сумісність операційних систем і апаратних засобів, портативність;

– відповідність затвердженому типу;

– технічне обслуговування і зміна конфігурації.

Документ регламентує процедуру затвердження типу та методи перевірки ПЗ, наведена програма випробувань ПЗ залежно від встановленого рівня ризику. Документи, які надає виробник ЗВТ (розробник ПЗ) під час затвердження типу, повинні містити відомості, достатні для перевірки відповідності вимогам документу OIML D 31 [1].

Рекомендація WELMEC 7.2 [4] встановлює загальні вимоги до ЗВТ з ПЗ. В першу чергу рекомендація орієнтована на об'єкти регулювання Директиви MID [6], яка гармонізована в Україні як відповідний ТР. Так як рекомендація носить загальний характер, вона може бути застосована також і для інших ЗВТ з ПЗ. Вимоги рекомендації стосуються лише ПЗ і не охоплюють технічні вимоги, що є індивідуальними для кожного виду ЗВТ. Вимоги повинні бути викладені у відповідних нормативно-правових документах.

Основним об'єктом рекомендації WELMEC 7.2 є ПЗ, але приділяється певна увага також і апаратній частині ЗВТ. Рекомендація має структурований набір блоків вимог, що складається з:

– вимог до базових конфігурацій ЗВТ (з вбудованим ПЗ – P, на базі універсального комп'ютера – U), а саме:

– до складу обов'язкових даних програмних документів, що надаються додатково до спеціальних документів, необхідних для опису реалізацій вимог до конфігурації та спеціальних вимог;

– щодо ідентифікації ПЗ і методів її захисту для високих рівнів ризику;

– щодо впливу через інтерфейс користувача;

– щодо впливу через інтерфейс зв'язку;

– щодо захисту від випадкових і ненавмисних змін;

– щодо захисту від навмисних змін;

– щодо захисту параметрів;

– щодо забезпечення справжності ПЗ (тільки для типу U);

– щодо унеможливлення впливу іншого ПЗ на роботу ЗВТ (тільки для типу U);

– вимог до конфігурацій вимірювальних технологій (довготривале зберігання – L, інтерфейс зв'язку – T, програмне розділення – S, завантаження оновлень – D), включаючи вимоги із захисту даних, що зберігаються та передаються, відновленню даних та виявлення помилок;

– спеціальних вимог до ЗВТ, що регулюються Директивою MID (лічильники води – I1, лічильники та перетворювачі об'єму газу – I2, лічильники активної електричної енергії – I3, лічильники кількості теплоти – I4, системи для безперервного та динамічного вимірювання об'єму рідин, крім води – I5, автоматичні ваги – I6, таксометри – I7).

Кожен із зазначених блоків має свою назву і містить чітко визначені вимоги, що його стосуються, пояснюючі коментарі, необхідні відомості у програмних документах, настанови щодо випробування та приклади прийнятних рішень. Обсяг вимог залежить від вибраного класу ризику. Рекомендація містить визначені класи ризику для деяких ЗВТ залежно від сфери застосування та рекомендації щодо визначення класу ризику для інших ЗВТ. Незмінне ПЗ має клас ризику А і, згідно з рекомендацією, не підлягає випробуванням.

Документи, які надає виробник ЗВТ (розробник ПЗ) під час затвердження типу, повинні містити відомості, достатні для перевірки відповідності вимогам рекомендації WELMEC 7.2.

6. Загальні вимоги національного стандарту щодо спеціального програмного забезпечення для засобів вимірювальної техніки

Національний стандарт ДСТУ 7363 встановлює загальні вимоги до ПЗ ЗВТ, інтегрованого та універсального, що може бути змінено в процесі експлуатації. Основним об'єктом стандарту є ПЗ ЗВТ.

Вимоги до ПЗ ЗВТ поділяються на такі:

– вимоги до структури з метою забезпечення проведення випробувань функцій ПЗ на відповідність вимогам стандарту та інших нормативних документів, відсутність впливу на них іншого ПЗ;

– вимоги до захисту ПЗ, а саме:

– захист від несанкціонованого доступу через програмні та апаратні інтерфейси;

– захист від збоїв та спотворень, що можуть порушити цілісність даних та результатів вимірювань;

– захист від ненавмисних та навмисних змін ПЗ;

– введення категорій користувачів з різними правами доступу;

– забезпечення контролю цілісності ПЗ;

– застосування ПЗ при його відповідності встановленим вимогам;

– вимоги до документування ПЗ.

Вимоги щодо ідентифікації, захищеності та придатності ПЗ ЗВТ встановлюються незалежно від рівнів випробувань, але обсяг випробувань та ступінь відповідності ПЗ встановленим вимогам залежить від визначеного рівня жорсткості. Стандарт містить рекомендацію щодо визначення рівня жорсткості. Крім того, рівень жорсткості випробувань можна визначити застосовуючи стандарт ISO/IEC 27005 [21]. При цьому рівень жорсткості буде відповідати встановленому рівню ризику.

7. Обговорення результатів щодо можливості спільного використання вимог міжнародних і регіональних документів на національному рівні

Порівняльний аналіз вимог і випробувань ПЗ згідно з вимогами стандарту ДСТУ 7363, документу OIML D 31 і рекомендації WELMEC 7.2 наведено у табл. 1.

Таблиця 1

Порівняльний аналіз вимог і випробування ПЗ

<table>
<tr><td rowspan="2">Вимоги щодо ПЗ</td><td colspan="3">Пункти та розділи НД</td></tr>
<tr><td>ДСТУ 7363</td><td>OIML D 31</td><td>WELMEC 7.2</td></tr>
<tr><td>1. Документування</td><td>4.4</td><td>6.1</td><td>P1, U1</td></tr>
<tr><td>2. Ідентифікація</td><td>4.3.7</td><td>5.1.1</td><td>P2, U2</td></tr>
<tr><td colspan="4">3. Захищеність</td></tr>
<tr><td colspan="4">3. 1. Цілісність ПЗ</td></tr>
<tr><td>– захист від випадкових та ненавмисних змін ПЗ</td><td>4.2.5</td><td>5.1.3.2</td><td>P5, U5</td></tr>
<tr><td>– захист від навмисних змін ПЗ</td><td>4.2.1, 4.2.5</td><td>5.1.3.2</td><td>P6, U6</td></tr>
<tr><td>– захист цілісності ПЗ та представлення результатів вимірювання</td><td>4.2.2, 4.2.5</td><td>5.1.4.2</td><td>U8</td></tr>
<tr><td colspan="4">3. 2. Інтерфейс користувача</td></tr>
<tr><td>– данні, що вводяться (клавіатура)</td><td rowspan="2">4.2.2*</td><td>5.1.3.2</td><td rowspan="2">P3, U3</td></tr>
<tr><td>– данні, що виводяться (дисплей)</td><td>5.1.3.1</td></tr>
<tr><td colspan="4">3. 3. Дані, що зберігаються</td></tr>
<tr><td>– захист від випадкових та ненавмисних змін даних, що зберігаються</td><td rowspan="6">4.2.6*</td><td>5.1.3.2,
5.2.3.1,</td><td>L2</td></tr>
<tr><td>– захист від навмисних змін даних, що зберігаються</td><td>5.2.3.2,</td><td>L3</td></tr>
<tr><td>– захист параметрів ПЗ</td><td>5.2.3.4</td><td>P7, U7</td></tr>
<tr><td>– достовірність даних вимірювань, що зберігаються</td><td>*</td><td>L4</td></tr>
<tr><td>– конфіденційність ключів</td><td>5.1.3.3</td><td>L5</td></tr>
<tr><td>– відновлення даних, що зберігаються</td><td>-</td><td>L6</td></tr>
<tr><td colspan="3">3. 4. Дані, що передаються через інтерфейс зв’язку</td><td>P4, U4</td></tr>
<tr><td>– захист від випадкових та ненавмисних змін даних, що передаються по мережам зв’язку</td><td rowspan="5">4.2.1, 4.2.2*</td><td>5.2.3.1,
5.2.3.2,</td><td>T2</td></tr>
<tr><td>– захист від навмисних змін даних, що передаються по мережам зв’язку</td><td>5.2.3.5,
5.2.3.6</td><td>T3</td></tr>
<tr><td>– достовірність даних вимірювань, що передаються по мережам зв’язку</td><td>*</td><td>T4</td></tr>
<tr><td>– конфіденційність ключів</td><td>5.1.3.3</td><td>T5</td></tr>
<tr><td>– дії з пошкодженими при передачі даними</td><td>*</td><td>T6</td></tr>
</table>

4. Придатність			
– функціональна відповідність (принцип функціонування)	4.3.4	5.1.2	*
– застосування за призначенням	4.3.2	5.1.3.1	L1, L7, L8, T1, T7, T8, Ix-3
– захист від впливу іншого ПЗ	4.1.2	5.2.4	U9
– обробка нестандартних ситуацій	4.2.3, 4.4.8, 4.4.9	5.1.4.1	Ix-1, Ix-4

*Примітка: * – вимога має загальний, непрямий характер або стосується всього розділу*

Національний стандарт ДСТУ 7363 не розглядає можливості розділення ПЗ на законодавчо значиму та не значиму частини, все ПЗ вважається законодавчо значимим. Також не розглядається можливість оновлення затвердженого ПЗ. Для кожної версії (або при зміні ідентифікації) необхідно проводити окремі випробування. Вимоги стандарту стосуються лише ПЗ, тому для перевірки ЗВТ необхідно застосовувати додатково відповідні стандарти та рекомендації, що стосуються конкретного виду ЗВТ.

ДСТУ 7363 встановлює критерії оцінювання відповідності ПЗ, але не містить методів проведення випробувань. Тобто він не дозволяє визначити рівень презумпції відповідності ПЗ вимогам ТР під час оцінювання відповідності ЗВТ. Для конкретизації вимог до ПЗ і забезпечення методики виконання випробувань необхідно додатково використовувати документи OIML D 31 та WELMEC 7.2.

Схематичне зображення застосування стандартів, документів і рекомендацій під час оцінювання відповідності ПЗ ТР наведено на рис. 3.

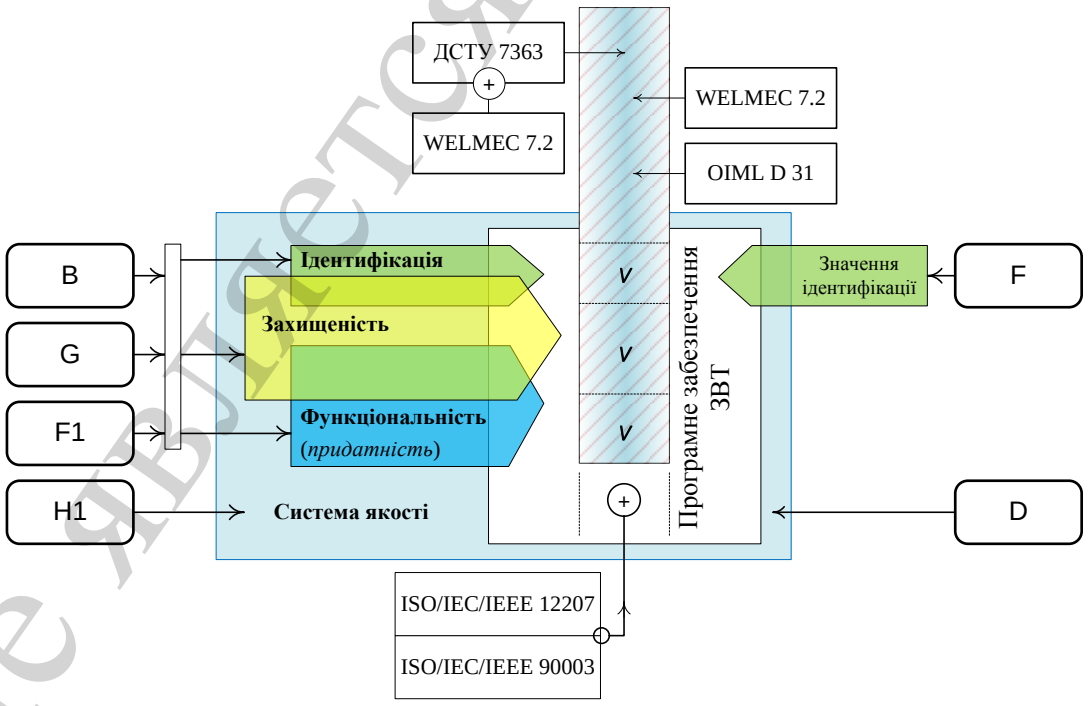

Рис. 3. Використання нормативних документів під час оцінювання відповідності ПЗ вимогам ТЗ щодо ЗВТ

Як видно з рис. 3, використання наведених нормативних документів під час оцінювання відповідності ЗВТ на відповідність вимогам ТР щодо ЗВТ за модулями B, F1 і G є достатнім, так як вони охоплюють ті ж вимоги до ПЗ, що і ТР. Під час використання модуля F перевіряють відповідність програмної ідентифікації, вказаної під час затвердження типу ЗВТ (модуль B), ніяких інших випробувань ПЗ не застосовують.

Під час використання модулів D і H1 виробнику ЗВТ додатково необхідно показати дотримання вимог щодо життєвого циклу ПЗ [22] і використовувати стандарти, що стосуються системи якості під час розробки ПЗ [23].

Презумпцію відповідності ПЗ ЗВТ вимогам ТР щодо ЗВТ дає:

– за модулями B, F1 і G – відповідність стандарту ДСТУ 7363, документу OIML D 31 або рекомендації WELMEC 7.2, яка підтверджена відповідними протоколами випробувань;

– за модулями D та H1 – додатково наявність підтвердження вимогам стандартів ISO/IEC/IEEE 12207 та ISO/IEC 90003.

Використання стандарту ДСТУ 7363 для випробувань ПЗ ЗВТ потребує додаткового використання документів міжнародних і регіональних організацій OIML і WELMEC з метою виконання вимог методики виконання випробувань.

На основі проведених досліджень та отриманих у табл. 1 даних запропоновано алгоритм проведення випробувань ПЗ ЗВТ з метою оцінки відповідності, який наведений на рис. 4.

Алгоритм побудований з врахуванням вимог документів міжнародної та регіональної організацій законодавчої метрології OIML і WELMEC, а також національного стандарту ДСТУ 7363. Крім того, у алгоритмі враховані вимоги міжнародних стандартів ISO/IEC/IEEE 12207 щодо життєвого циклу ПЗ і ISO/IEC 90003 щодо системи якості під час розробки ПЗ. Як видно із рис. 4 найбільший обсяг випробувань проводиться під час оцінювання ЗВТ за модулями D і H1, декілька менший – за модулями B, F1 і G, а найменший (лише перевірка програмної ідентифікації) – за модулем F. Таким чином застосування запропонованого алгоритму проведення випробувань ПЗ ЗВТ дозволяє врахувати всі необхідні елементи, достатні для досягнення презумпції відповідності ПЗ суттєвим вимогам ТР.

З використанням запропонованого алгоритму (рис. 4) розроблені спеціальні контрольні переліки для перевірки ПЗ за кожним із вказаних модулів. Такі контрольні переліки є аналогами переліків, наведених в документі WELMEC 7.2 [4, 11] і застосовуються для конкретних ЗВТ, призначених для застосування у сфері законодавчо регульованої метрології. З використанням розроблених спеціальних контрольних переліків орган з оцінки відповідності ДП «Укрметртестстандарт» лише у 2018 році провів випробування ПЗ ЗВТ за модулем B (одним із найбільш поширених модулів) для біля 100 типів ЗВТ, а за модулем F – біля сотні тисяч одиниць ЗВТ.

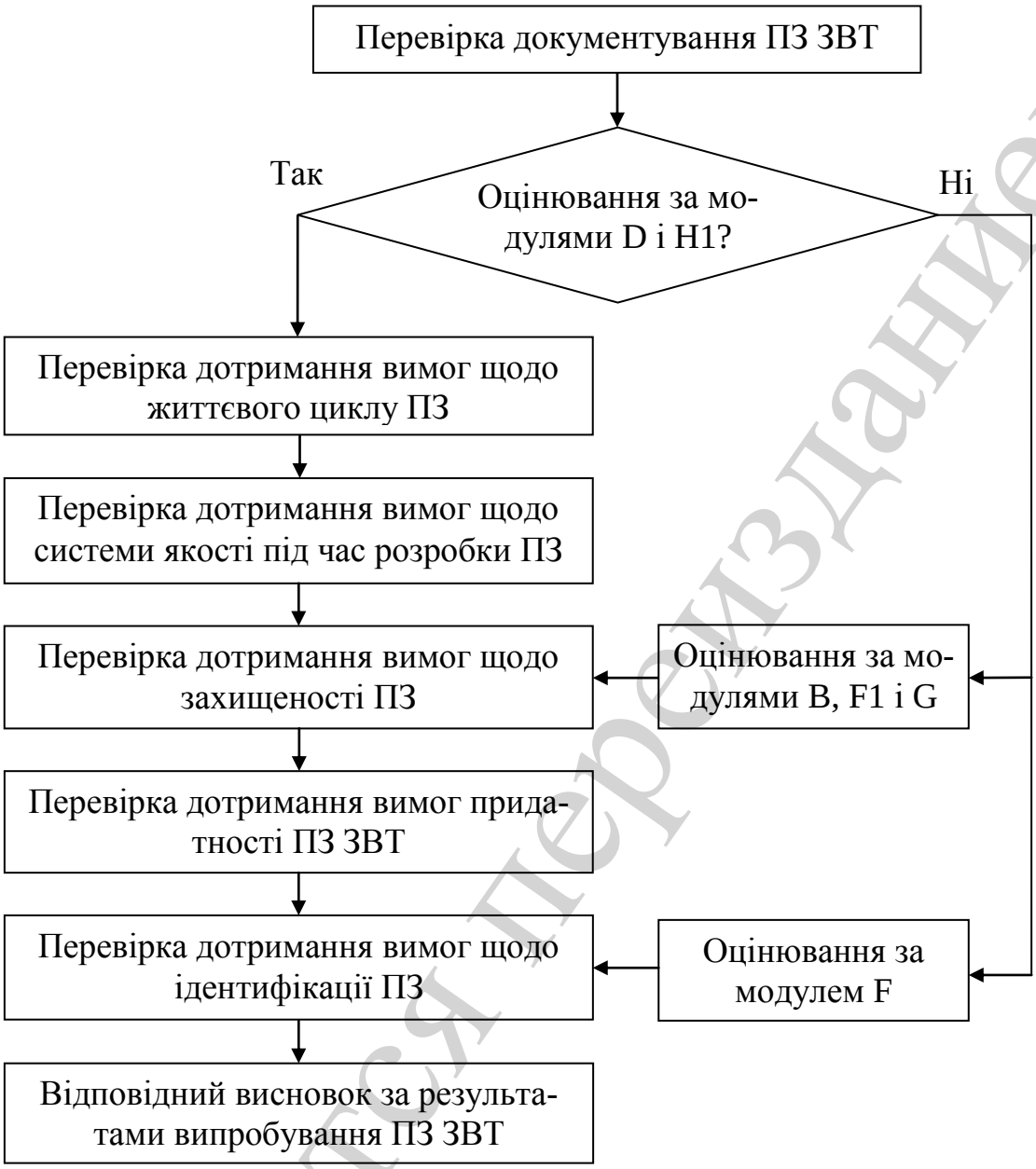

Рис. 4. Пропонований алгоритм проведення випробувань ПЗ ЗВТ з метою оцінки відповідності

Наразі загальні технічні вимоги до ПЗ ЗВТ та процедуру оцінювання відповідності суттєвим вимогам ТР на національному рівні регламентує лише національний стандарт ДСТУ 7363, яким не визначена методологія проведення випробувань ПЗ. Проведені дослідження можуть бути використанні під час перегляду ДСТУ 7363 та розробленні нового національного стандарту на його заміну з урахуванням положень документів міжнародної та регіональної організацій законодавчої метрології OIML і WELMEC.

8. Висновки

1. Проведено порівняльний аналіз положень національних нормативних документів і документів міжнародної та регіональної організацій OIML і

WELMEC щодо випробування ПЗ ЗВТ на відповідність суттєвим вимогам ТР щодо ЗВТ. Зокрема стосовно придатності ПЗ до застосування та захисту від несанкціонованого втручання. Встановлено, що наявний національний стандарт ДСТУ 7363 містить загальні вимоги щодо захисту ПЗ і не визначає методології проведення випробувань ПЗ.

2. Встановлені та досліджені необхідні елементи, достатні для досягнення презумпції відповідності ПЗ суттєвим вимогам ТР під час оцінювання відповідності ЗВТ. Визначена необхідність додаткового застосування міжнародних і регіональних документів OIML D 31 або WELMEC 7.2 для конкретизації вимог до ПЗ ЗВТ і WELMEC 7.2 для забезпечення методики виконання випробувань ПЗ ЗВТ. Необхідність додаткового використання документів міжнародної та регіональної організацій OIML і WELMEC під час випробування ПЗ для ЗВТ доводить потребу перегляду національного стандарту ДСТУ 7363.

3. Встановлений та досліджений алгоритм проведення випробувань ПЗ для ЗВТ з метою оцінки відповідності з урахуванням вимог документів міжнародної та регіональної організацій законодавчої метрології OIML і WELMEC, а також національного стандарту ДСТУ 7363. Алгоритм враховує вимоги міжнародних стандартів ISO/IEC/IEEE 12207 щодо життєвого циклу ПЗ і ISO/IEC 90003, що стосуються системи якості під час розробки ПЗ. Це дозволить враховувати всі необхідні елементи, достатні для досягнення презумпції відповідності ПЗ суттєвим вимогам ТР.

Література

1. OIML D 31:2008. General Requirements for Software Controlled Measuring Instruments. OIML. Paris, 2008. 53 p.
2. COOMET R/LM/10:2004. COOMET Recommendation: Software for Measuring Instruments: General Technical Specifications. COOMET, 2004. 10 p.
3. WELMEC 7.1. Informative Document: Development of Software Requirements. URL: http://www.welmec.org/fileadmin/user_files/publications/WG_07/7-1_FRPO.pdf
4. WELMEC 7.2. Software Guide (Measuring Instruments Directive 2004/22/EC). URL: http://www.welmec.org/fileadmin/user_files/publications/WG_07/Guide_7.2_2015__Software.pdf
5. WELMEC 2.3. Guide for Examining Software (Non-automatic Weighing Instruments). URL: http://www.welmec.org/fileadmin/user_files/publications/2-3.pdf
6. Directive 2014/32/EU on the harmonisation of the laws of the Member States relating to the making available on the market of measurement instrument (recast) // Official Journal of the European Union. 2004. L96/149. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0032
7. Velichko O. N. Normative base for certification of measurement provision software // Measurement Techniques. 2007. Vol. 50, Issue 4. P. 364–371. doi: https://doi.org/10.1007/s11018-007-0076-5
8. Velychko O., Gordiyenko T. The implementation of general international guides and standards on regional level in the field of metrology // Journal of Phys-

ics: Conference Series. 2010. Vol. 238. P. 012044. doi: https://doi.org/10.1088/1742-6596/238/1/012044

9. Velichko O. N. Basic tests, stages, and features in monitoring measuring instrument software // Measurement Techniques. 2009. Vol. 52, Issue 6. P. 566–571. doi: https://doi.org/10.1007/s11018-009-9308-1

10. Velychko O. Using of Validated Software for Uncertainty Analyses Tools in Accredited Laboratories // Key Engineering Materials. 2008. Vol. 381-382. P. 599–602. doi: https://doi.org/10.4028/www.scientific.net/kem.381-382.599

11. Velychko O., Gordiyenko T., Hrabovskyi O. Testing of measurement instrument software on the national level // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 2, Issue 9 (92). P. 13–20. doi: https://doi.org/10.15587/1729-4061.2018.125994

12. Achieving Software Security for Measuring Instruments under Legal Control / Peters D., Grottker U., Thiel F., Peter M., Seifert J.-P. // Position Papers of the 2014 Federated Conference on Computer Science and Information Systems. 2014. Vol. 3. P. 123–130. doi: https://doi.org/10.15439/2014f460

13. Esche M., Thiel F. Software Risk Assessment for Measuring Instruments in Legal Metrology // Proceedings of the 2015 Federated Conference on Computer Science and Information Systems. 2015. Vol. 5. P. 1113–1123. doi: https://doi.org/10.15439/2015f127

14. Software risk assessment and evaluation process (SRAEP) using model based approach / Sadiq M., Rahmani M. K. I., Ahmad M. W., Jung S. // 2010 International Conference on Networking and Information Technology. 2010. doi: https://doi.org/10.1109/icnit.2010.5508535

15. Software evaluation of smart meters within a Legal Metrology perspective: A Brazilian case / Boccardo D. R., dos Santos L. C. G., da Costa Carmo L. F. R., Dezan M. H., Machado R. C. S., de Aguiar Portugal S. // 2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe). 2010. doi: https://doi.org/10.1109/isgteurope.2010.5638881

16. A Secure System Architecture for Measuring Instruments in Legal Metrology / Peters D., Peter M., Seifert J.-P., Thiel F. // Computers. 2015. Vol. 4, Issue 2. P. 61–86. doi: https://doi.org/10.3390/computers4020061

17. IT Security standards and legal metrology – Transfer and Validation / Thiel F., Hartmann V., Grottker U., Richter D. // EPJ Web of Conferences. 2014. Vol. 77. P. 00001. doi: https://doi.org/10.1051/epjconf/20147700001

18. Jacobson J. Validation of software in measuring instruments // Computer Standards & Interfaces. 2006. Vol. 28, Issue 3. P. 277–285. doi: https://doi.org/10.1016/j.csi.2005.07.006

19. Thiel F., Grottker U., Richter D. The challenge for legal metrology of operating systems embedded in measuring instruments // OIML Bull. 2011. Vol. 52, Issue 1. P. 5–14.

20. ДСТУ 7363:2013. Програмне забезпечення засобів вимірювальної техніки. Загальні технічні вимоги. Київ: Мінекономрозвитку України, 2013. 11 с.

21. ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management. International Organization for Standardization, 2018. 56 p.

22. ISO/IEC/IEEE 12207:2017. Systems and software engineering. Software life cycle processes. International Organization for Standardization, 2017. 145 p.

23. ISO/IEC/IEEE 90003:2018. Software engineering. Guidelines for the application of ISO 9001:2008 to computer software. International Organization for Standardization, 2018. 69 p.